Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A method for defence against ~~at least one~~ an attack made by means of differential power analysis ~~in at least one hyperelliptic cryptosystem, in particular in at least one~~, the method comprising:

randomizing at least one factor in a hyperelliptic public key cryptosystem, which is given by at least one hyperelliptic curve of any genus over a finite field in a first group, where the hyperelliptic curve is given by at least one coefficient, ~~characterised in that~~ wherein the factor is selected from the group consisting of:

the hyperelliptic curve ~~and/or~~; and

at least one element of the first group~~, in particular at least one in particular reduced divisor and/or at least one intermediate result of a scalar multiplication is randomised~~.

2. (currently amended) A method as claimed in claim 1, ~~characterised in that the~~ wherein bits of the operand to be processed ~~and/or~~ or encoded in the hyperelliptic public key cryptosystem are represented by ~~the hyperelliptic curve, in particular by~~ at least one co-efficient of the hyperelliptic curve~~, and/or by at least one base element of the cryptosystem, such as by at least one in particular reduced divisor and/or at least one intermediate result of a scalar multiplication~~.

3. (currently amended) A method as claimed in claim 1, ~~characterised in that~~ wherein at least one scalar multiplication in ~~the~~ a Jacobian variation of the hyperelliptic curve takes place in a second group different from the first group and isomorphic in relation to the first group, in particular selected at random.

4. (currently amended) A method as claimed in claim 3, ~~characterised by the following steps~~ further comprising:

~~transformation of~~ transforming the Jacobian variation of the hyperelliptic curve ~~by means of at least one depiction~~, ~~in particular~~ by means of at least one K-isomorphism, into the Jacobian variation of the transformed hyperelliptic curve;

~~multiplication of~~ multiplying the Jacobian variation of the transformed hyperelliptic curve with at least one scalar; and

~~back transformation of~~ transforming the Jacobian variation multiplied by the scalar ~~(n)~~ of the transformed hyperelliptic curve ~~)by~~ by means of the depiction inverse to the depiction in ~~a~~ Jacobian variations of the hyperelliptic curve multiplied by scalars, where the depiction corresponds to the transition from the first group to the second group and the inverse depiction corresponds to the transition from the second group to the first group.

5. (currently amended) A method as claimed in claim 1, ~~characterised by the following steps~~ further comprising:

~~depiction of~~ depicting at least one ~~in particular~~ reduced divisor with an associated polynomial pair as at least one quintuplet in projective co-ordinates, where $U(t)=t^2+U_1t/Z+U_0/Z$ and $V(t)=V_1t/Z+V_0/Z$;

~~selection, in particular random selection, of~~ randomly selecting at least one non-vanishing element from the field; and

~~conversion of~~ converting the quintuplet by means of a selected element into ~~the~~ a converted quintuplet.

6. (currently amended) A method as claimed in claim 1, ~~characterised by the following steps~~ further comprising:

~~depiction of~~ depicting at least one ~~in particular~~ reduced divisor with associated polynomial pair as at least one sextuplet a projective co-ordinates, where $U(t)=t^2+U_1t/Z_1^2+U_0/Z_1^2$ and $V(t)=V_1t/(Z_1^3Z^2)+V_0/(Z_1^3Z_2)$;

~~selection, in particular random selection, of~~ randomly selecting at least two non-vanishing elements from the field; and

~~conversion of~~ converting the sextuplet by means of a selected elements into ~~the~~ a converted sextuple.

7. (currently amended) A method as claimed in claim 1, ~~characterised in that~~ further comprising implementing the method ~~is implemented on at least one~~ on a microprocessor ~~in particular allocated to at least one chip card and/or in particular to at least one~~ of a smart card.

8. (currently amended) A microprocessor to implement instructions for defence against at least one attack made by means of differential power analysis in at least one hyperelliptic public key cryptosystem, which is given by at least one hyperelliptic curve of any genus over a finite field in a first group, where the hyperelliptic curve is given by at least one coefficient, wherein the microprocessor is configured to randomize at least one factor selected from the group consisting of the hyperelliptic curve and at least one element of the first group ~~working according to a method as claimed in claim 1~~.

9. (currently amended) A ~~device, in particular a chip card and/or in particular a~~ smart card, the smart card comprising ~~with~~ at least one microprocessor as claimed in claim 8.

10. (currently amended) Use of a method as claimed in claim 1 ~~and/or at least one microprocessor as claimed in claim 8 and/or at least one dvice in particular at least one chip card and/or at least one smart card as claimed in claim 9~~ in the defence against at least one attack made by means of differential power analysis on at least one hyperelliptic ~~cryptosystem, in particular at least one~~ public key cryptosystem.

11. (new) The method of claim 1, wherein randomizing at least one element of the first group comprises randomizing at least one reduced divisor.

12. (new) The method of claim 1, wherein randomizing at least one element of the first group comprises randomizing at least one intermediate result of a scalar multiplication.

13. (new) The method of claim 1, wherein bits of the operand to be processed and/or encoded in the hyperelliptic public key cryptosystem are represented by at least one base element of the cryptosystem, wherein the base element comprises at least one reduced divisor, at least one intermediate result of a scalar multiplication, or at least one of each of the reduced devisor and the intermediate result of the scalar multiplication.